Por Naturaleza, WordPress Y Otros CMS Son Inseguros

Actualmente encontramos gran contenido en la web, lo que muchos ignoran, es que estos son administrados por gestores de contenido (CMS) como **WordPress** y otros CMS. En los blogs personales, particularmente podemos encontrar el uso de un CMS, ha sido tal la popularidad de los gestores de contenido, que se han adoptado en grandes empresas para hacer **presencia en la web**. Los CMS se usan debido a que permiten una facilidad al momento de publicar los artículos, facilitan la contribución por parte de diversos autores, y permite dar ciertos permisos que deseemos a determinados usuarios. Sin duda, la funciones que brinda un CMS son bastante impresionantes, si deseas algo mas, puedes contar con la ayuda de complementos ó extensiones, pero CUIDADO! Estas grandes ayudas, también permiten **vulnerar un sitio web**.

Los expertos en seguridad informática de High-Tech Bridge con frecuencia descubren vulnerabilidades en extensiones y plugins para los **CMS mas populares**. Es un procedimiento estándar para notificar al desarrollador antes de lanzar algo al publico, esto proporciona una oportunidad para que los problemas sean solucionados sin alertar a los atacantes quienes podrían aprovecharlos. El CEO de High-Tech Bridge, **Ilia Kolochenko**, dice que los problemas de seguridad de la CMS no son nada nuevo:

> *«Por más de una década las principales plataformas CMS como Joomla y WordPress han sido profundamente investigados por hackers de sombrero blanco y negro. En los primeros días, las inyecciones SQL y los defectos de ejecución de código eran algo común. De hecho, alrededor del **90 por ciento de los sitios web** eran vulnerables a los ataques críticos de riesgo*

que permiten tomar el control de la página web de forma remota dentro de pocos minutos «.

Una gran cantidad de trabajo se ha puesto en asegurar que los **CMS** son seguros una vez instalados, lo que lleva a Kolochenko a decir: «Yo diría que un popular CMS, como **WordPress o Joomla** puede considerarse seguro en la instalación por defecto, si se configuran correctamente, no tienen código de terceros y están actualizados».

Pero ahí radica el problema. Comienzas a añadir extensiones, y esto se vuelve en una historia muy diferente. **High Bridge Tech** señala que muchos plugins son desarrollados por programadores sin experiencia que carecen de conocimientos necesarios para garantizar la seguridad. La falla de seguridad en los plugins puede ser al menos tan grave como cualquiera que pudiera haber existido en el CMS a sí mismos en el pasado. «Mediante la explotación de XSS y fallas en SQLi, el atacante puede obtener la contraseña de administrador como si estuviera explotando estas vulnerabilidades en el código del núcleo de la aplicación web».